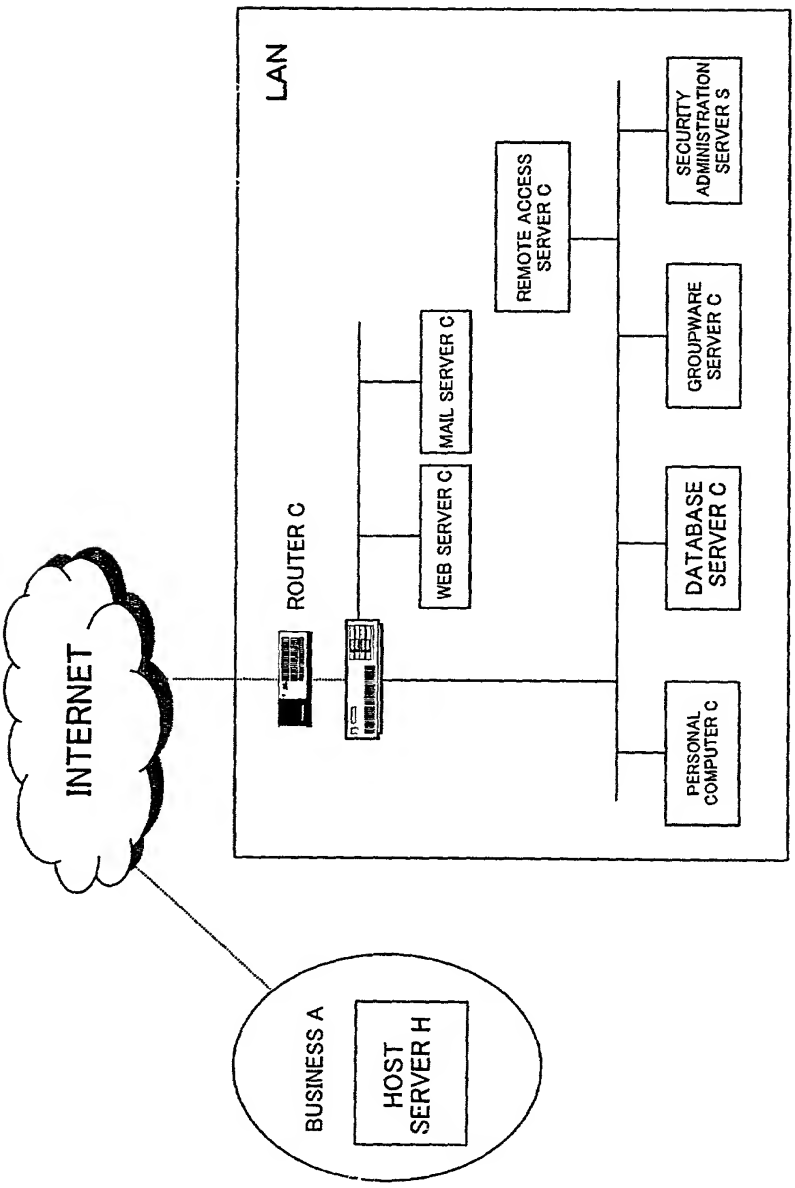

INTERNET
BUSINESS A
HOST SERVER H
LAN
ROUTER C
WEB SERVER C
MAIL SERVER C
REMOTE ACCESS SERVER C
DATABASE SERVER C
GROUPWARE SERVER C
SECURITY ADMINISTRATION SERVER S
PERSONAL COMPUTER C

FIG. 1

RELIABILITY
LOW
HIGH
ACCESS AND USER'S USE HISTORY
INTERNET
RELATED COMPANIES
INTRAOFFICE
IN BUILDING
IN DEPARTMENT
RELEVANT CLOSED LAN
11
13
15
17
SEGMENT OBJECT 15
LONG BROKEN LINE : REMOTE CONTROL
SHORT BROKEN LINE : FILE TRANSFER
SOLID LINE : BOTH REMOTE CONTROL AND FILE TRANSFER
CUBE OBJECT 13 : USER
SPHERE OBJECT 11 : COMPUTER
TETRAHEDRON OBJECT 17 : PRIVILEGED COMMAND EXECUTION USER

FIG. 2

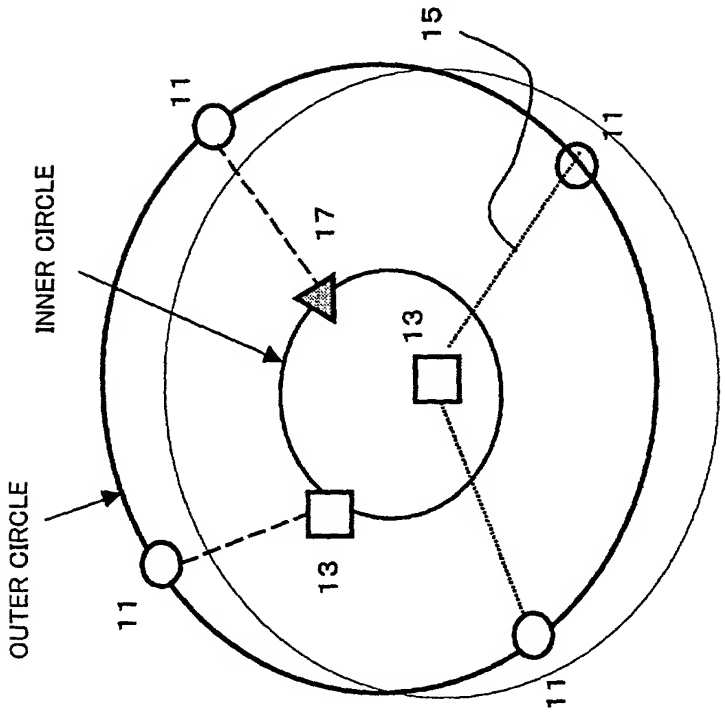


FIG. 3

DEVICE TO BE MONITORED		DISPLAY METHOD OF LAYERS (GROUP CLASSIFICATION)				DISPLAY TIME		OPERATION OF DISPLAY ANGLE	
		FOR EACH DOMAIN	FOR EACH DEPARTMENT	FOR EACH BUILDING FLOOR	FOR EACH ACCESS TYPE	REAL TIME	PLAYBACK	DEFAULT	ARBITRARY
1	PERSONAL COMPUTER			O		O			O
2	DATA BASE SERVER				O	O			O
3	WEB SERVER	O				O		O	
4	MAIL SERVER		O				O	O	
5									
6									
7									
8									
9									
10									

SETTING ENVIRONMENT		OS				DHCP ENVIRONMENT		LOG COLLECTION TIME	
		unix	unix	unix	Windows	OPEN	SEER DHCP	5 MINS.	ARBITRARY
1	PERSONAL COMPUTER	O					O	O	
2	DATA BASE SERVER	O					O	O	
3	WEB SERVER			O		O		O	
4	MAIL SERVER			O		O			240MINS
5									
6									
7									
8									
9									
10									

FIG. 4

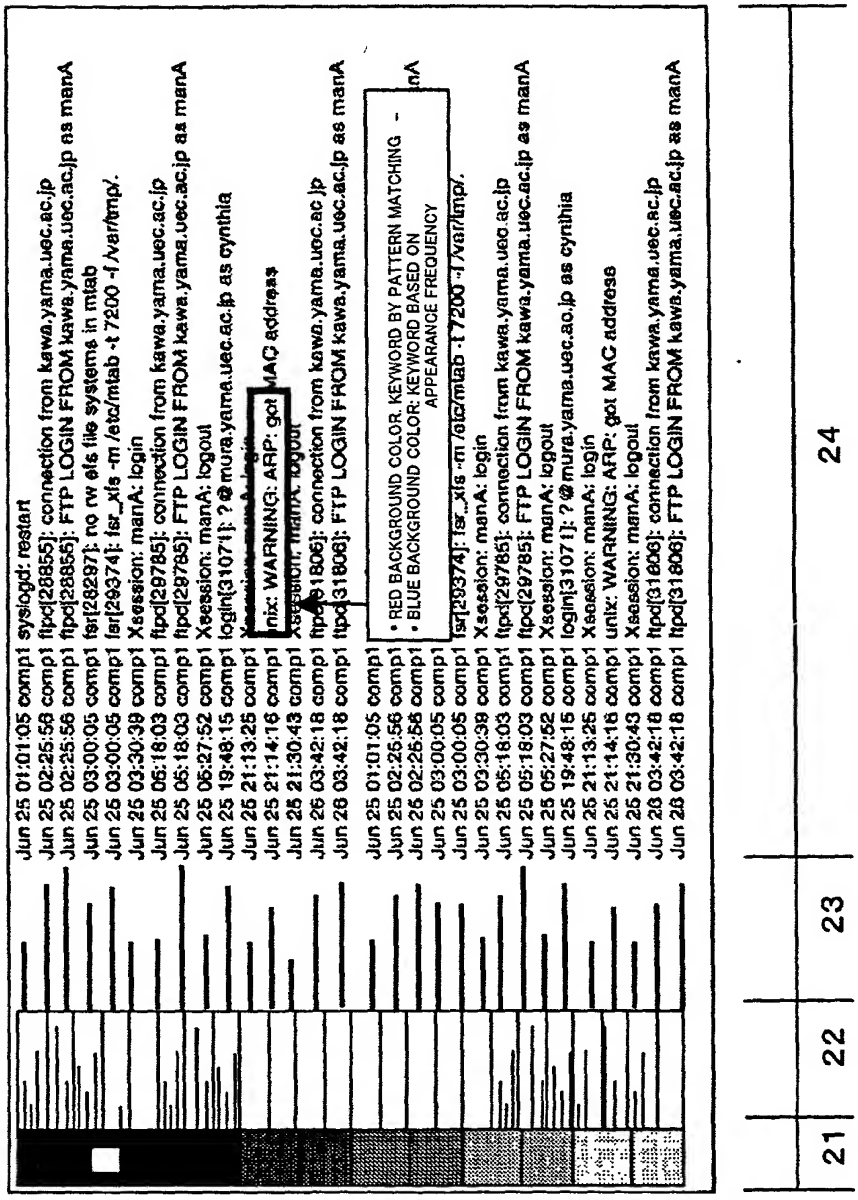

Jun 25 01:01:05 comp1 syslogd: restart
Jun 25 02:25:56 comp1 ftpd[28855]: connection from kawa.yama.uec.ac.jp
Jun 25 02:25:56 comp1 ftpd[28855]: FTP LOGIN FROM kawa.yama.uec.ac.jp as manA
Jun 25 03:00:05 comp1 fsr[28297]: no rw efs file systems in mtab
Jun 25 03:00:05 comp1 fsr[29374]: fsr_xfs -m /etc/mtab -t 7200 -f /var/tmp/.
Jun 25 03:30:39 comp1 Xsession: manA: login
Jun 25 05:18:03 comp1 ftpd[29785]: connection from kawa.yama.uec.ac.jp
Jun 25 05:18:03 comp1 ftpd[29785]: FTP LOGIN FROM kawa.yama.uec.ac.jp as manA
Jun 25 05:27:52 comp1 Xsession: manA: logout
Jun 25 19:48:15 comp1 login[31071]: ?@mura.yama.uec.ac.jp as cynthia
Jun 25 21:13:25 comp1
Jun 25 21:14:16 comp1 unix: WARNING: ARP: got MAC address
Jun 25 21:30:43 comp1 Xsession: manA: logout
Jun 26 03:42:18 comp1 ftpd[31806]: connection from kawa.yama.uec.ac.jp
Jun 26 03:42:18 comp1 ftpd[31806]: FTP LOGIN FROM kawa.yama.uec.ac.jp as manA
Jun 25 01:01:05 comp1
Jun 25 02:25:56 comp1
Jun 26 02:26:58 comp1
Jun 25 03:00:05 comp1
Jun 25 03:00:05 comp1 fsr[29374]: fsr_xfs -m /etc/mtab -t 7200 -f /var/tmp/.
Jun 25 03:30:39 comp1 Xsession: manA: login
Jun 25 05:18:03 comp1 ftpd[29785]: connection from kawa.yama.uec.ac.jp
Jun 25 05:18:03 comp1 ftpd[29785]: FTP LOGIN FROM kawa.yama.uec.ac.jp as manA
Jun 25 05:27:52 comp1 Xsession: manA: logout
Jun 25 19:48:15 comp1 login[31071]: ?@mura.yama.uec.ac.jp as cynthia
Jun 25 21:13:25 comp1 Xsession: manA: login
Jun 25 21:14:16 comp1 unix: WARNING: ARP: got MAC address
Jun 25 21:30:43 comp1 Xsession: manA: logout
Jun 26 03:42:18 comp1 ftpd[31806]: connection from kawa.yama.uec.ac.jp
Jun 26 03:42:18 comp1 ftpd[31806]: FTP LOGIN FROM kawa.yama.uec.ac.jp as manA
• RED BACKGROUND COLOR: KEYWORD BY PATTERN MATCHING
• BLUE BACKGROUND COLOR: KEYWORD BASED ON APPEARANCE FREQUENCY
21
22
23
24

FIG. 5

XXX CORPORATION | CSO :TORU MUKAI | SYSTEM ADMINISTRATOR: MASAHIRO ADACHI

COMPUTER TO BE MONITORED		SPECIFICATION	SERVICE CONTENT			
		OS/CPU	BASIC FUNCTION	3D VISUALIZATION	REMOTE MONITORING	LOG CONCEALMENT
1	DBS SERVER 1	Solar	O	O	O	O
2	DBS SERVER 2	Solar	O	O	O	O
3	Web SERVER	Linux/ 1C	O	O	O	O
4	MAIL SERVER	Linux/ 1C	O	O	O	O
5	RAS Gateway	Solar	-	O	-	O
6						
7						

● OPERATING STATE OF ADMINISTRATION SERVER

OPERATING STATE	INSTALLMENT PLACE	COMPUTER TO BE ADMINISTERED				
		1	2	3	4	5
1 NORMAL	PRESIDENT'S ROOM	DBS SERVER 1	DBS SERVER 2	Web SERVER	MAIL SERVER	
2 NORMAL	INFORMATION ADMINISTRATION ROOM	REMOTE GATEWAY				
3						
4						
5						

FIG. 6

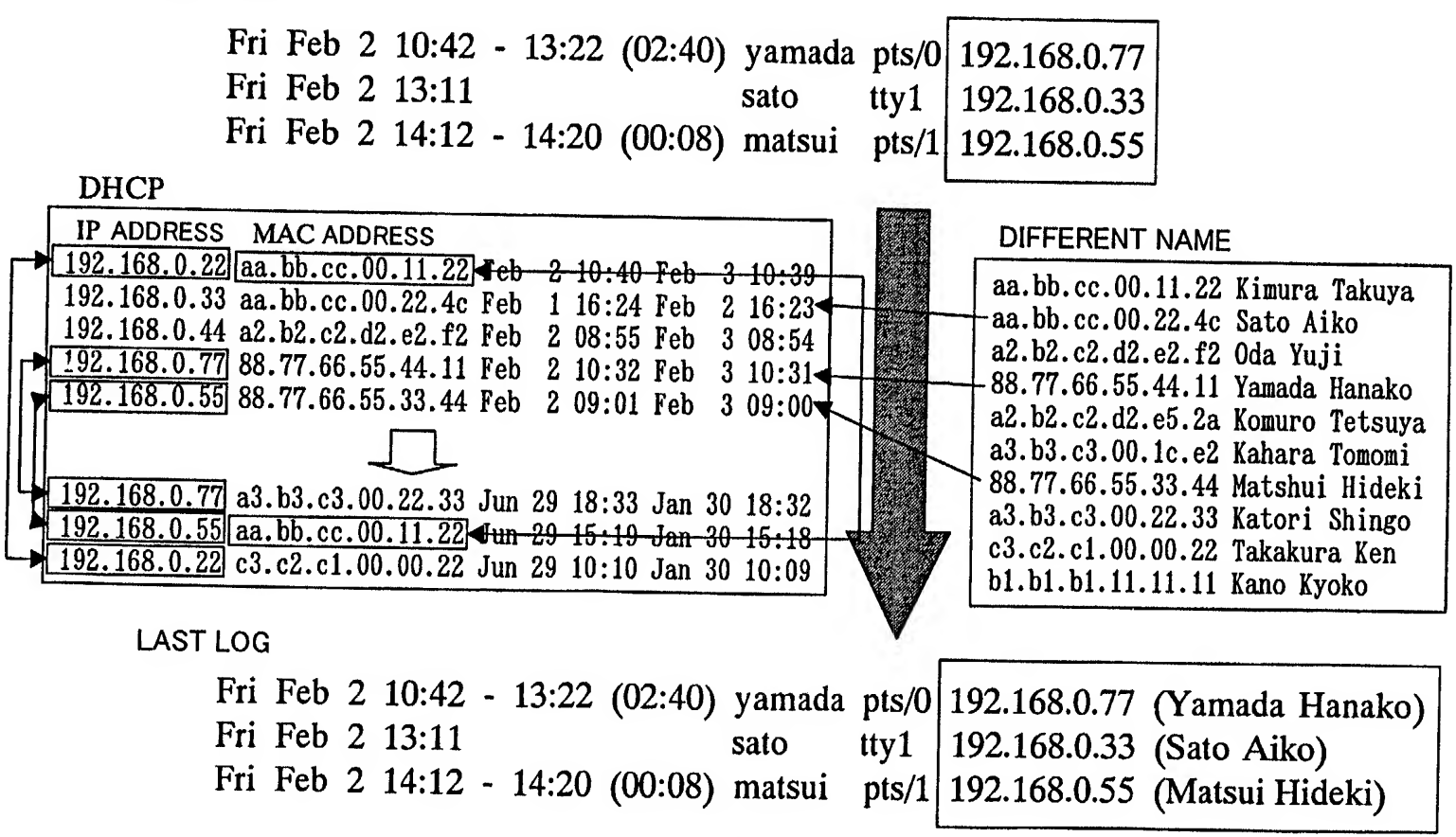


FIG. 7

Title: Secuity Administrative Server and Its Host Server
Inventor: Toru Mukai et al.
Atty. Ref. No.: 2430-000001

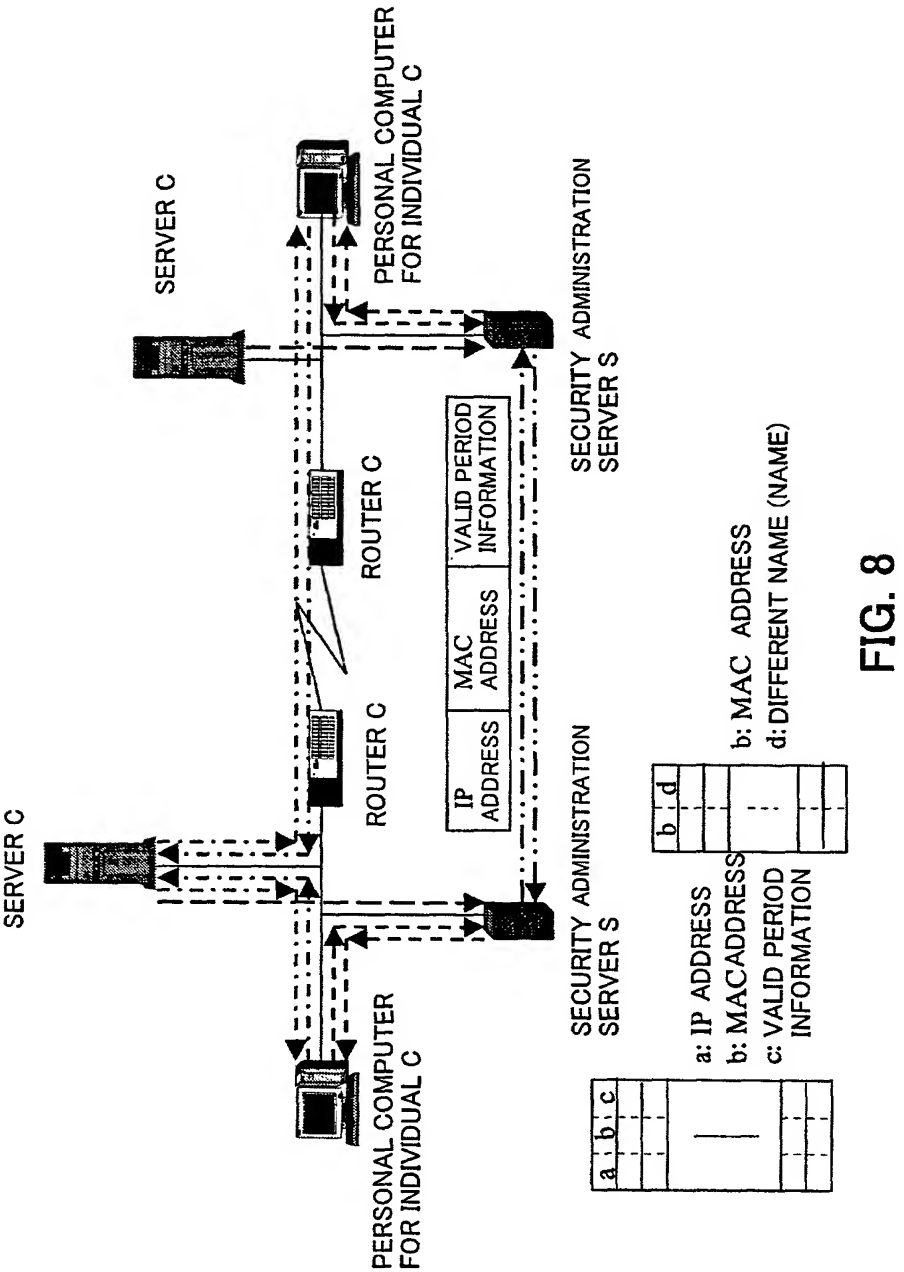

SERVER C
SERVER C
PERSONAL COMPUTER FOR INDIVIDUAL C
ROUTER C
ROUTER C
IP ADDRESS
MAC ADDRESS
VALID PERIOD INFORMATION
SECURITY ADMINISTRATION SERVER S
SECURITY ADMINISTRATION SERVER S
PERSONAL COMPUTER FOR INDIVIDUAL C
a: IP ADDRESS
b: MACADDRESS
c: VALID PERIOD INFORMATION
b: MAC ADDRESS
d: DIFFERENT NAME (NAME)

FIG. 8

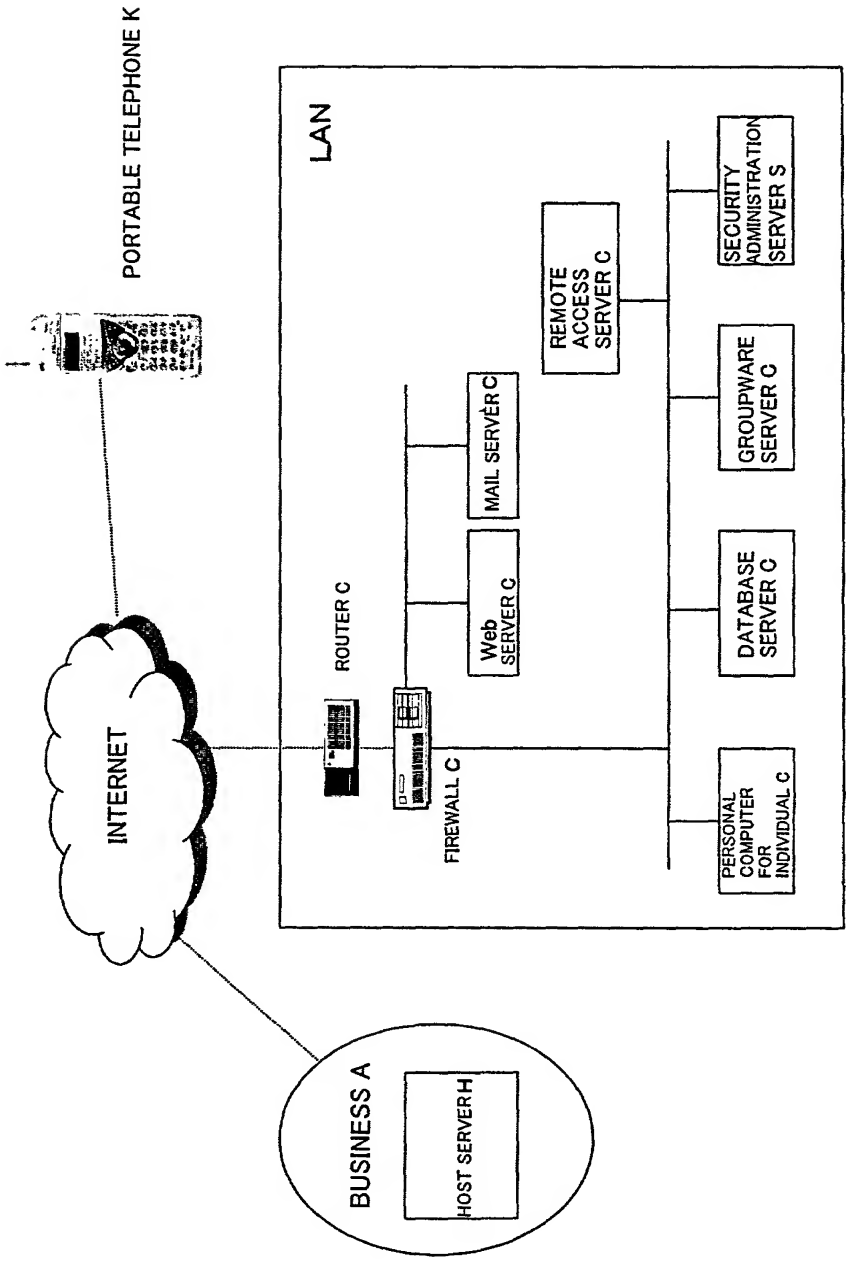

PORTABLE TELEPHONE K
LAN
INTERNET
ROUTER C
FIREWALL C
Web SERVER C
MAIL SERVER C
REMOTE ACCESS SERVER C
DATABASE SERVER C
GROUPWARE SERVER C
SECURITY ADMINISTRATION SERVER S
PERSONAL COMPUTER FOR INDIVIDUAL C
BUSINESS A
HOST SERVER H

FIG. 9

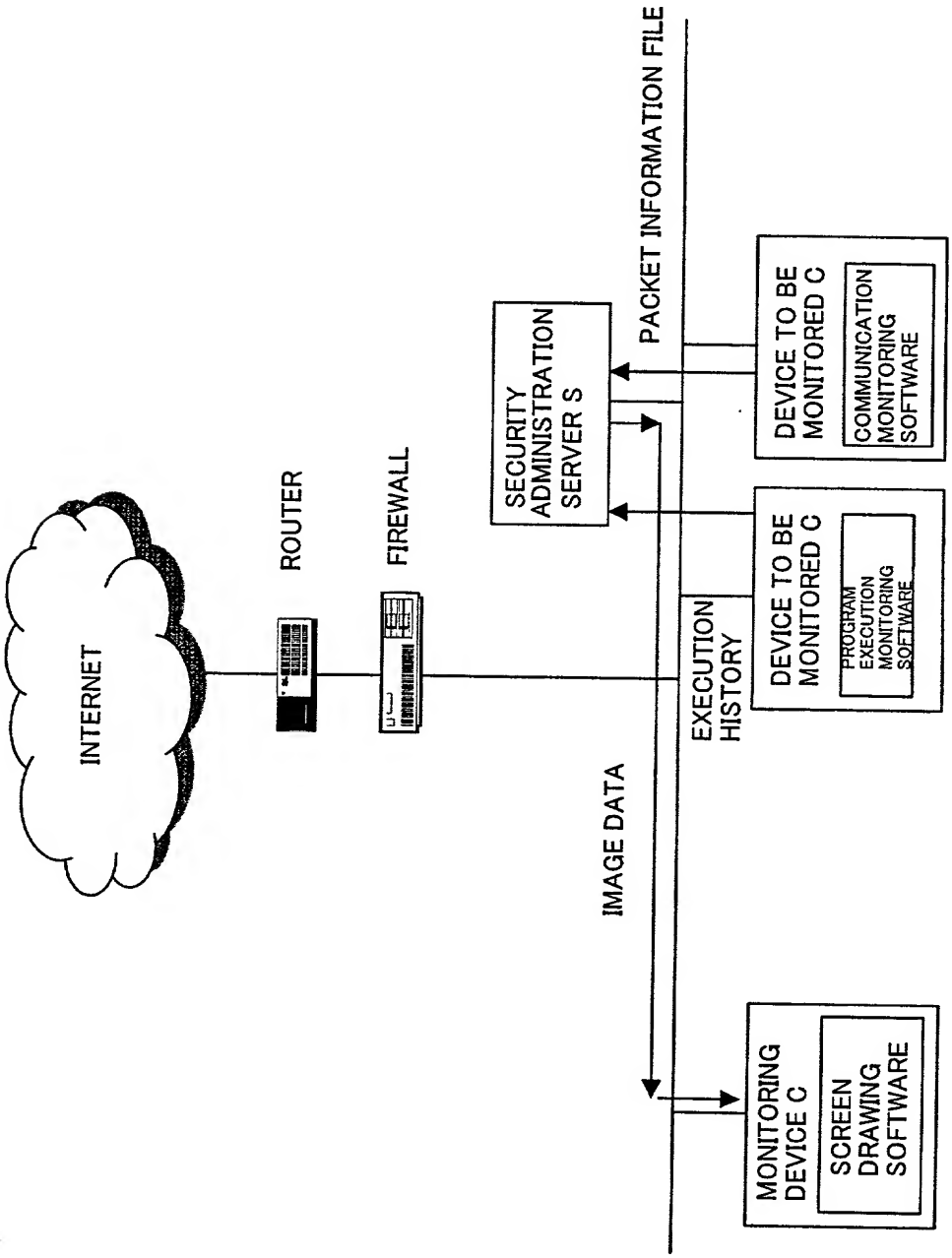
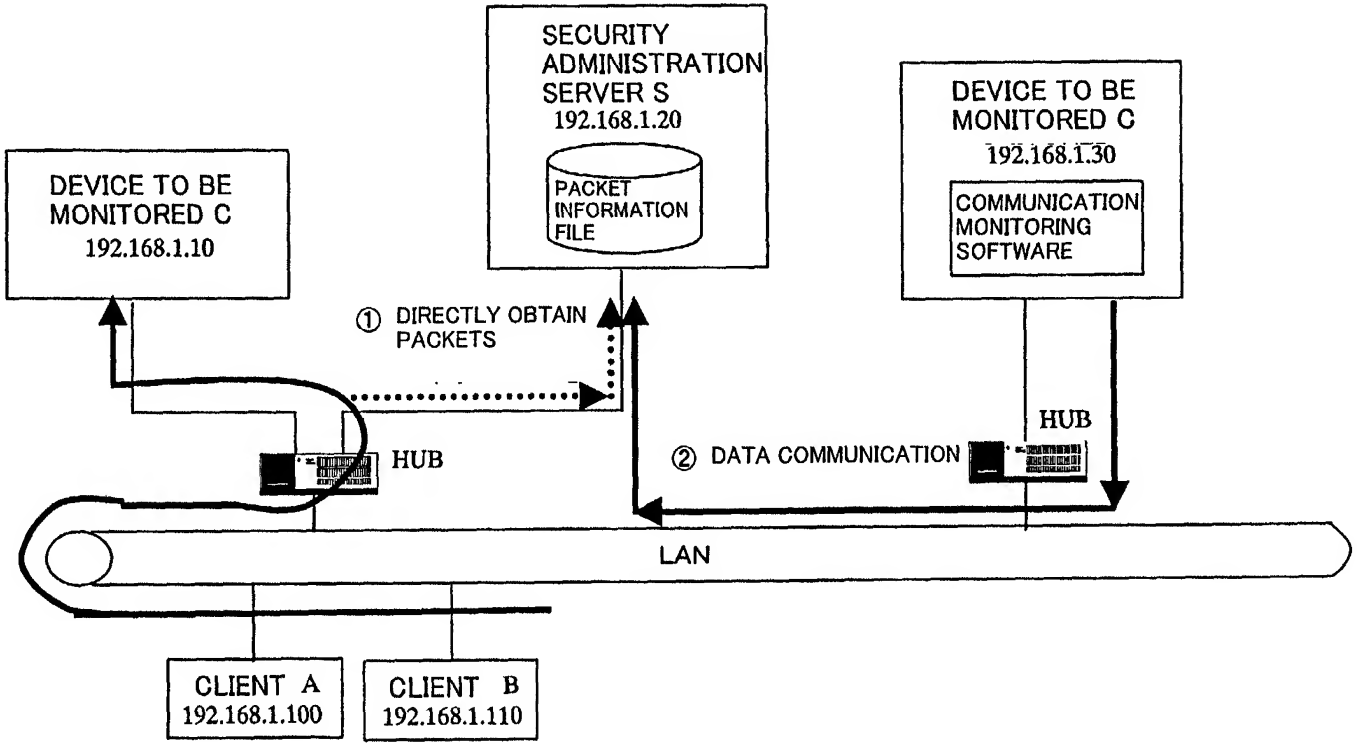

INTERNET
ROUTER
FIREWALL
SECURITY ADMINISTRATION SERVER S
PACKET INFORMATION FILE
DEVICE TO BE MONITORED C
COMMUNICATION MONITORING SOFTWARE
DEVICE TO BE MONITORED C
PROGRAM EXECUTION MONITORING SOFTWARE
EXECUTION HISTORY
IMAGE DATA
MONITORING DEVICE C
SCREEN DRAWING SOFTWARE

FIG. 10



①COMMMUNICATION PACKETS OF DEVICE TO BE MONITORED C CONNECTED TO THE SAME HUB AS SECURITY ADMINISTRATION SERVER S ARE DIRECTLY OBTAINABLE

②COMMUNICATION PACKETS OF DEVICE TO BE MONITORED C CONNECTED TO A DIFFERENT HUB THAN SECURITY ADMINISTRATION SERVER S, ARE ACCUMULATED AND STORED AT DEVICE TO BE MONITORED C SIDE, AND CONCENTRATED SUITABLY TO SECURITY ADMINISTRATION SERVER S BY DATA COMMUNICATION VIA LAN.

FIG. 11

DATA FORMAT OF PACKET INFORMATION FILE

FIELD NAME	DESCRIPTION
time	COLLECTION TIME (SERVER TIME)
btFlags	0:IN 1:OUT (FROM SERVER) 2:SMB (SUCH AS COMMON FILE ACCESS)
wLength	ORIGINAL LENGTH OF PACKET
mwMac	CLIENT MAC ADDRESS
dwIPAddr	CLIENT IP ADDRESS
wPort	SERVER PORT NUMBER
btDataLength	LENGTH OF PORTION OF VARIABLE DATA OF PACKET (0 TO 255)
btData[256]	VARIABLE DATA OF 256 PACKETS (VARIABLE LENGTH)

FIG. 12

BADIC VISUALIZATION DATA

FIELD NAME	DESCRIPTION
time	COLLECTING TIME (TIME AT SECURITY ADMINSTRATION SERVER)
wServerID	IDENTIFIER OF SERVER TO BE MONITORED
wType	TYPE OF PACKET (01:Login...65:Mail...)
mwMac	CLIENT MAC ADDRESS
dwIPAddr	CLIENT IP ADDRESS
wOriginalLength	ORIGINAL LENGTH OF PACKET
btData[256]	CHARACTER DATA FOR EACH TYPE OF 256 PACKETS (Login:UserID/Mail:from.to...)

FIG. 13

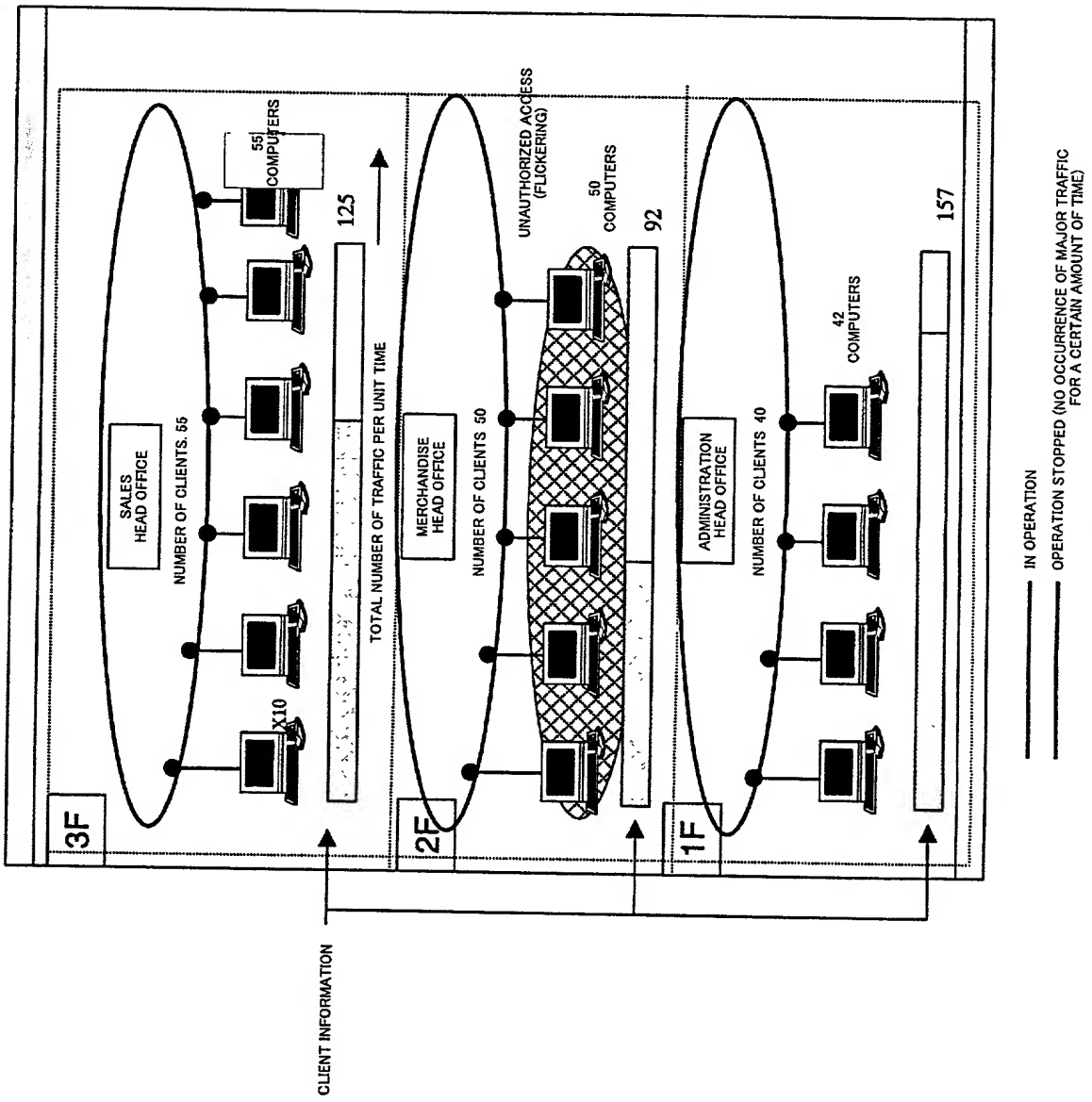

3F
SALES HEAD OFFICE
NUMBER OF CLIENTS. 55
55 COMPUTERS
X10
125
TOTAL NUMBER OF TRAFFIC PER UNIT TIME
2F
MERCHANDISE HEAD OFFICE
NUMBER OF CLIENTS 50
UNAUTHORIZED ACCESS (FLICKERING)
50 COMPUTERS
92
1F
ADMINISTRATION HEAD OFFICE
NUMBER OF CLIENTS 40
42 COMPUTERS
157
CLIENT INFORMATION
IN OPERATION
OPERATION STOPPED (NO OCCURRENCE OF MAJOR TRAFFIC FOR A CERTAIN AMOUNT OF TIME)

FIG. 14

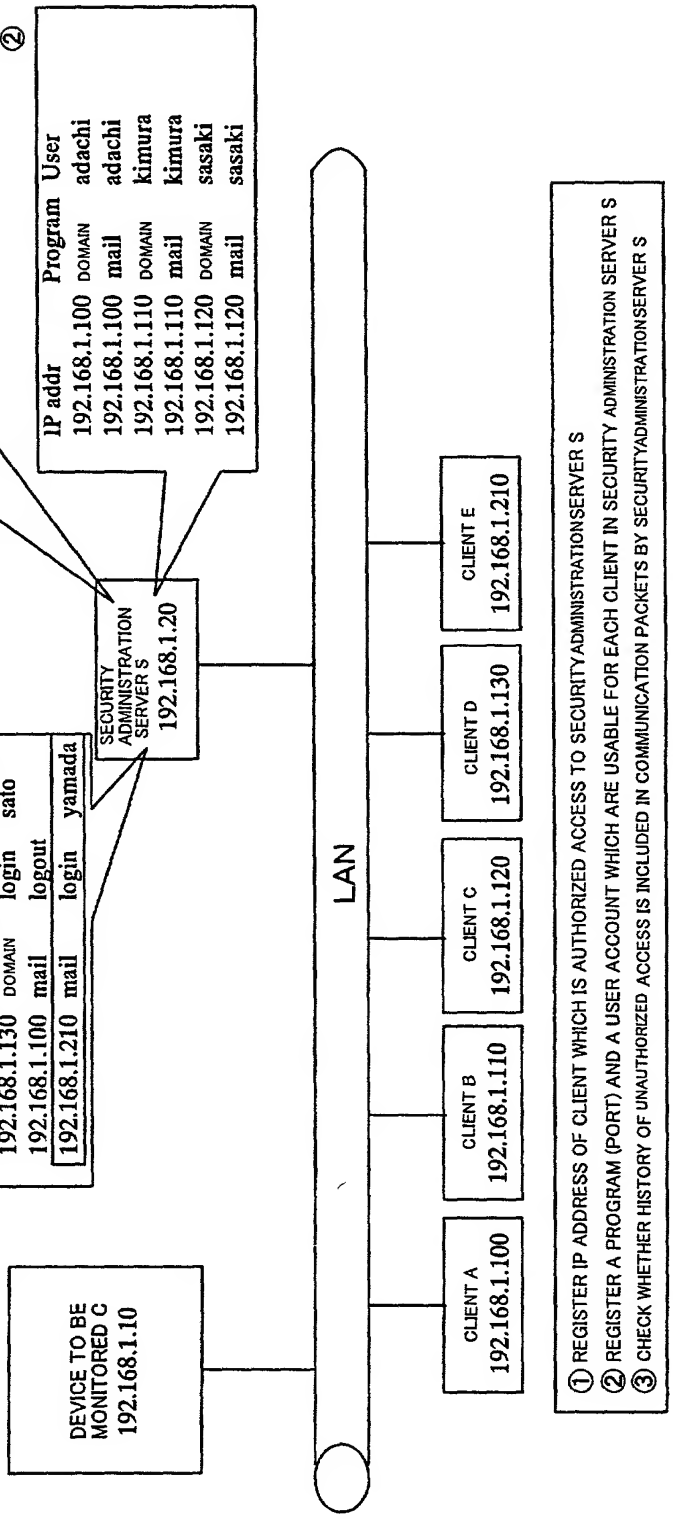

①
SERVER :192.168.1.10
192.168.1.100 – 192.168.1.150
②
IP addr Program User
192.168.1.100 DOMAIN adachi
192.168.1.100 mail adachi
192.168.1.110 DOMAIN kimura
192.168.1.110 mail kimura
192.168.1.120 DOMAIN sasaki
192.168.1.120 mail sasaki
③
IP addr Program Login User
192.168.1.100 mail login adachi
192.168.1.120 DOMAIN login suzuki
192.168.1.130 DOMAIN login sato
192.168.1.100 mail logout
192.168.1.210 mail login yamada
SECURITY ADMINISTRATION SERVER S
192.168.1.20
LAN
DEVICE TO BE MONITORED C
192.168.1.10
CLIENT A
192.168.1.100
CLIENT B
192.168.1.110
CLIENT C
192.168.1.120
CLIENT D
192.168.1.130
CLIENT E
192.168.1.210
① REGISTER IP ADDRESS OF CLIENT WHICH IS AUTHORIZED ACCESS TO SECURITY ADMINISTRATION SERVER S
② REGISTER A PROGRAM (PORT) AND A USER ACCOUNT WHICH ARE USABLE FOR EACH CLIENT IN SECURITY ADMINISTRATION SERVER S
③ CHECK WHETHER HISTORY OF UNAUTHORIZED ACCESS IS INCLUDED IN COMMUNICATION PACKETS BY SECURITY ADMINISTRATION SERVER S

FIG. 15

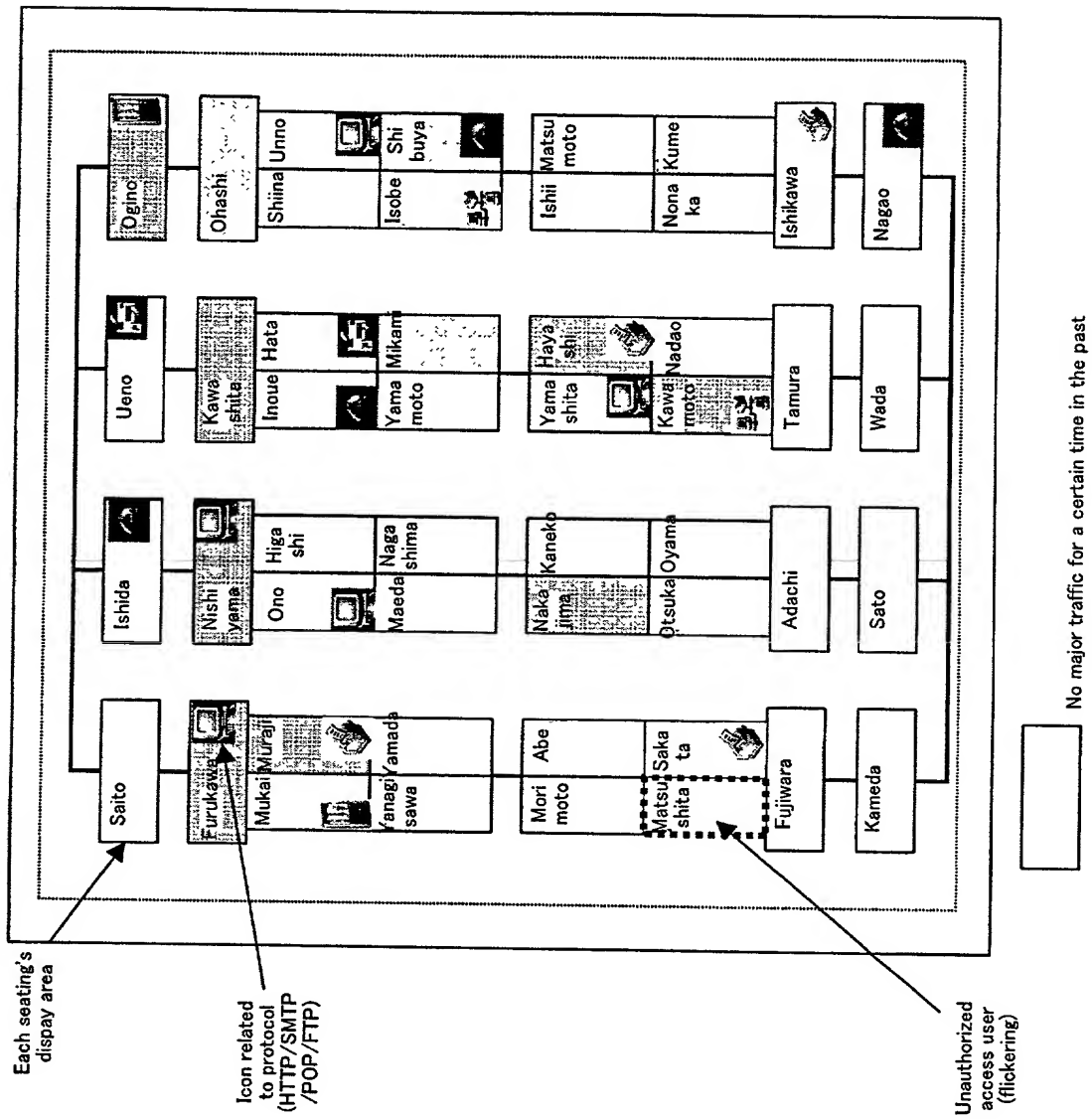

Each seating's dispay area
Icon related to protocol (HTTP/SMTP /POP/FTP)
Unauthorized access user (flickering)
No major traffic for a certain time in the past
Ogino
Ohashi
Shiina
Unno
Isobe
Shi buya
Ishii
Matsu moto
Nona ka
Kume
Ishikawa
Nagao
Ueno
Kawa shita
Inoue
Hata
Yama moto
Mikami
Yama shita
Haya shi
Kawa moto
Nadao
Tamura
Wada
Ishida
Nishi yama
Ono
Higa shi
Maeda
Naga shima
Naka jima
Kaneko
Otsuka
Oyama
Adachi
Sato
Saito
Furukawa
Mukai
Muraji
Yanagi sawa
Yamada
Mori moto
Abe
Matsu shita
Saka ta
Fujiwara
Kameda

FIG. 16

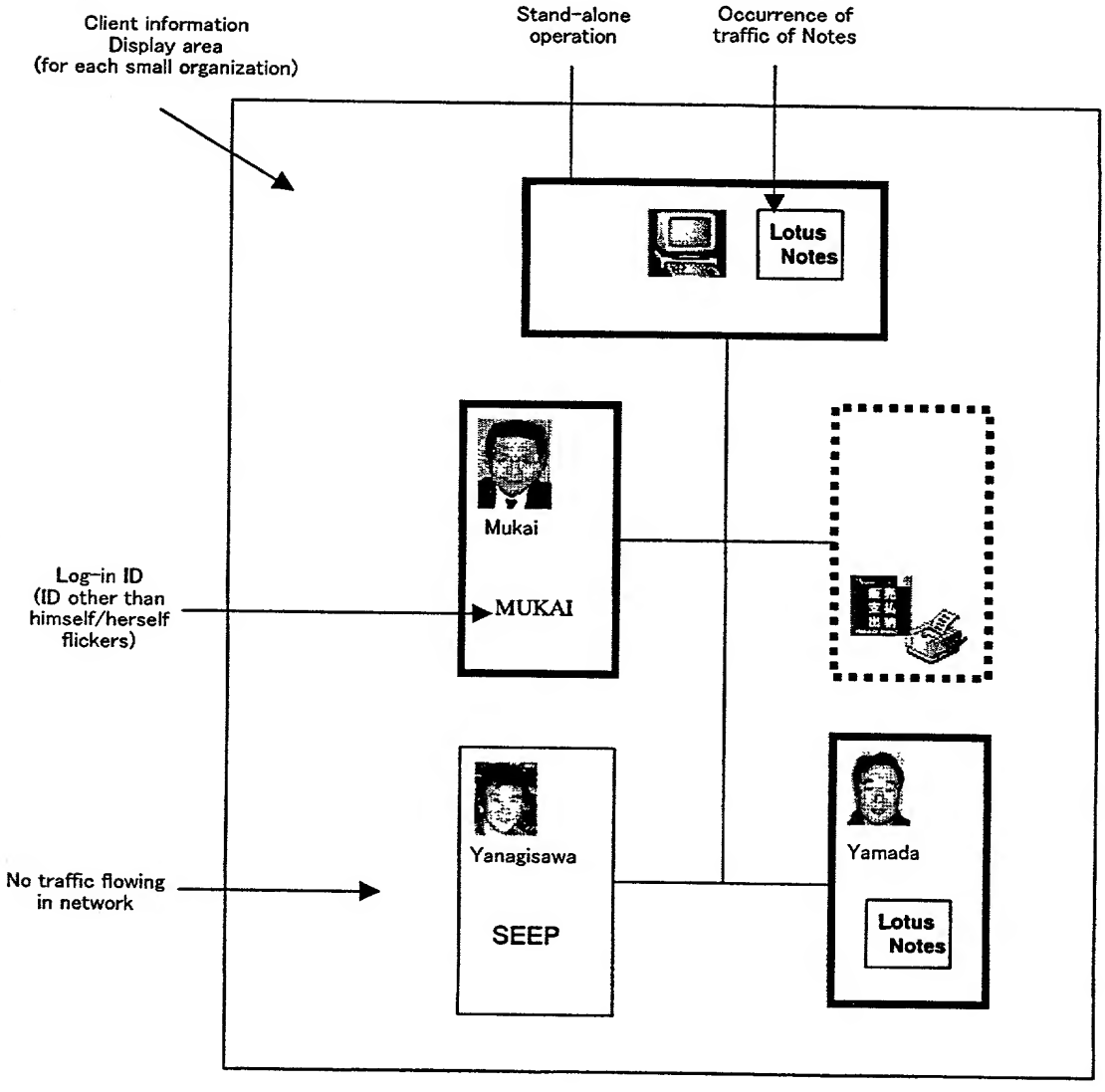

Client information
Display area
(for each small organization)
Stand-alone
operation
Occurrence of
traffic of Notes
Lotus
Notes
Mukai
MUKAI
Log-in ID
(ID other than
himself/herself
flickers)
Yanagisawa
SEEP
No traffic flowing
in network
Yamada
Lotus
Notes

FIG. 17

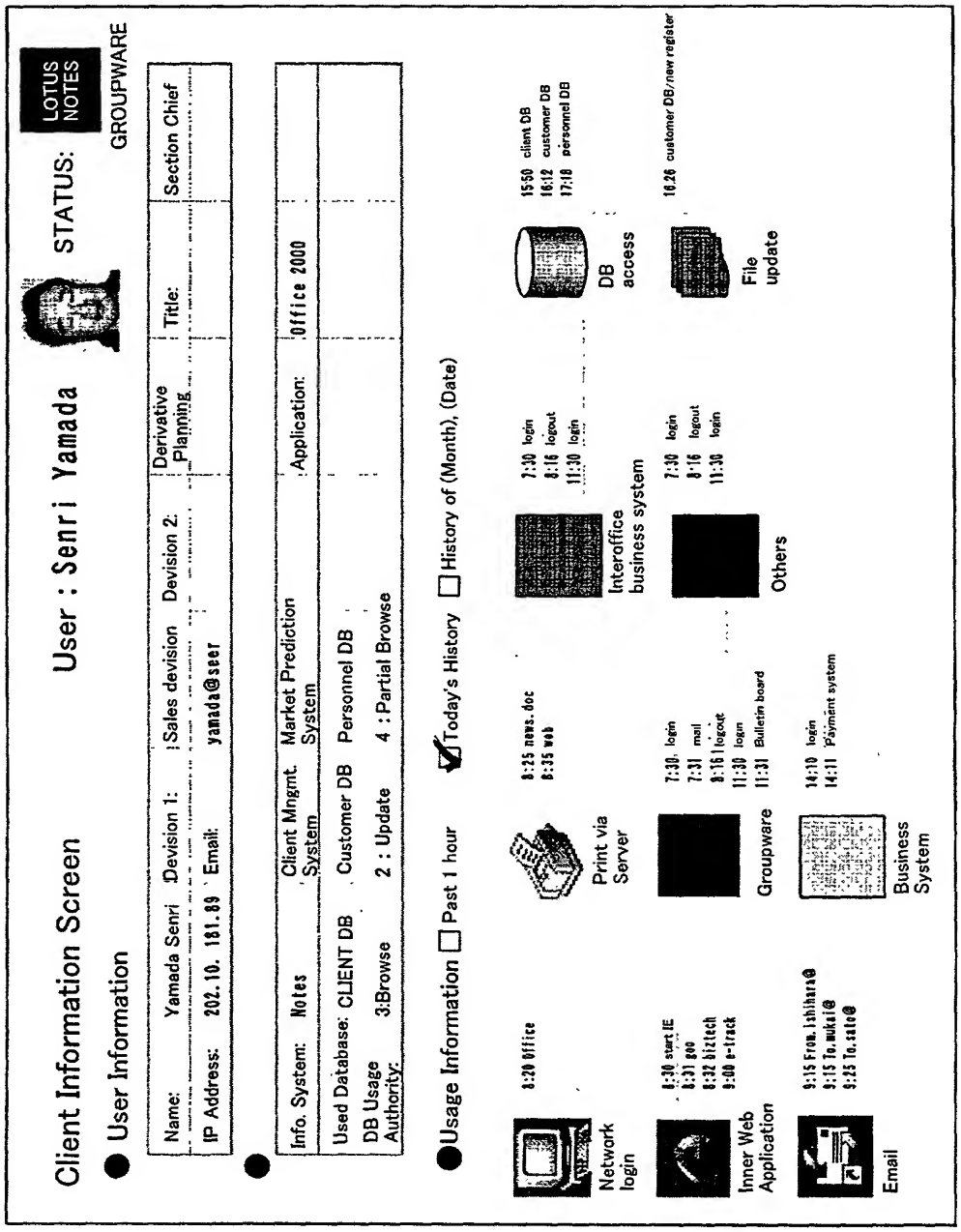

Client Information Screen
User : Senri Yamada
STATUS:
LOTUS NOTES
GROUPWARE
User Information
Name: Yamada Senri
Devision 1: Sales devision
Devision 2:
Derivative Planning
Title:
Section Chief
IP Address: 202.10. 181.89
Email: yamada@seer
Info. System: Notes
Client Mngmt. System
Market Prediction System
Application: Office 2000
Used Database: CLIENT DB
Customer DB
Personnel DB
DB Usage Authority:
3:Browse
2 : Update
4 : Partial Browse
Usage Information
Past 1 hour
Today's History
History of (Month), (Date)
8:20 Office
Network login
8:25 news. doc
8:35 web
Print via Server
7:30 login
8:16 logout
11:30 login
Interoffice business system
15:50 client DB
16:12 customer DB
17:18 personnel DB
DB access
8:30 start IE
8:31 goo
8:32 biztech
9:00 e-track
Inner Web Application
7:30. login
7:31 mail
8:16 logout
11:30 login
11:31 Bulletin board
Groupware
7:30 login
8:16 logout
11:30 login
Others
10:20 customer DB/new register
File update
9:15 From. ishihara@
9:15 To. mukai@
9:25 To. sato@
Email
14:10 login
14:11 Payment system
Business System

FIG. 18

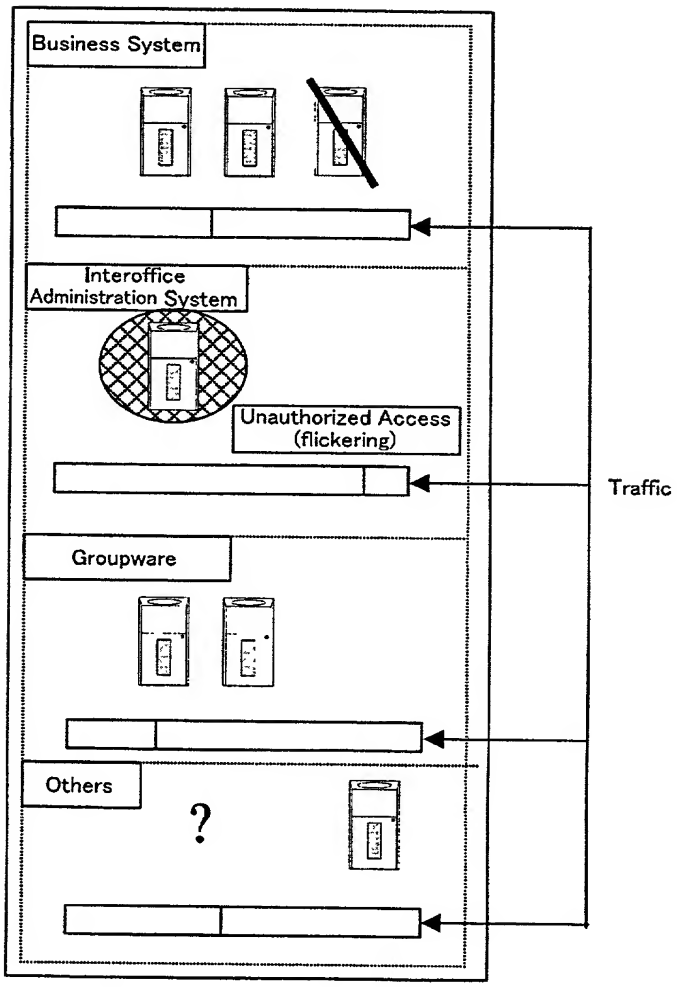

Business System
Interoffice
Administration System
Unauthorized Access
(flickering)
Traffic
Groupware
Others
?

FIG. 19

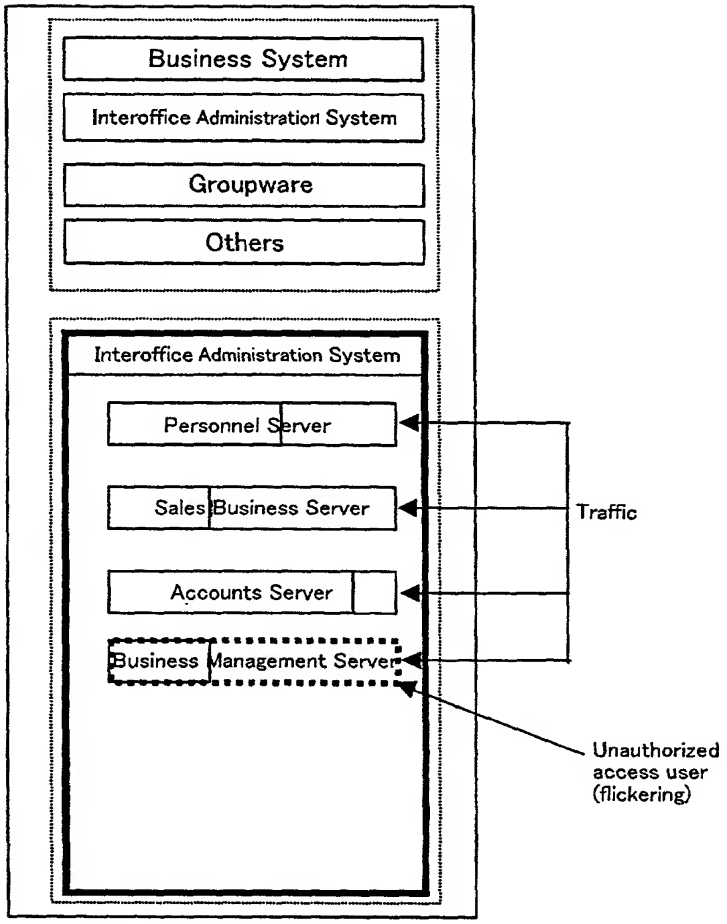

Business System
Interoffice Administration System
Groupware
Others
Interoffice Administration System
Personnel Server
Sales Business Server
Accounts Server
Business Management Server
Traffic
Unauthorized access user (flickering)

FIG. 20

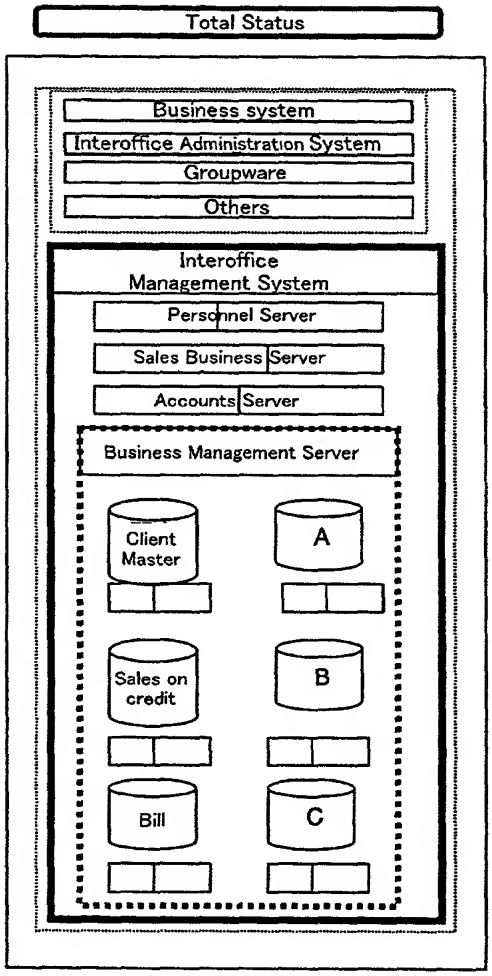

Total Status
Business system
Interoffice Administration System
Groupware
Others
Interoffice Management System
Personnel Server
Sales Business Server
Accounts Server
Business Management Server
Client Master
A
Sales on credit
B
Bill
C

FIG. 21

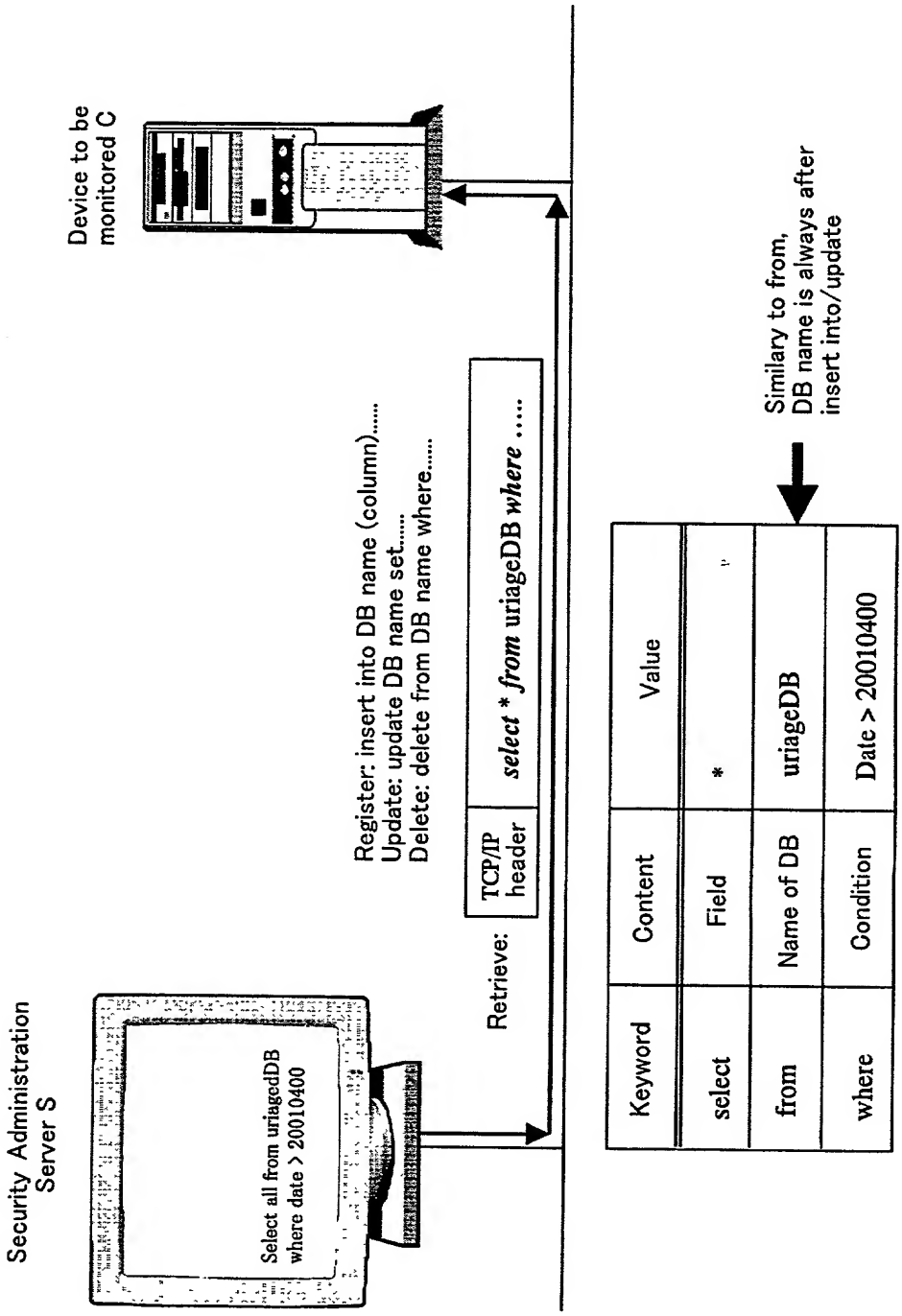

Device to be monitored C
Security Administration Server S
Select all from uriagedDB where date > 20010400
Retrieve:
TCP/IP header
select * from uriageDB where .....
Register: insert into DB name (column).....
Update: update DB name set.....
Delete: delete from DB name where.....
Similary to from, DB name is always after insert into/update
Keyword
Content
Value
select
Field
*
from
Name of DB
uriageDB
where
Condition
Date > 20010400

FIG. 22